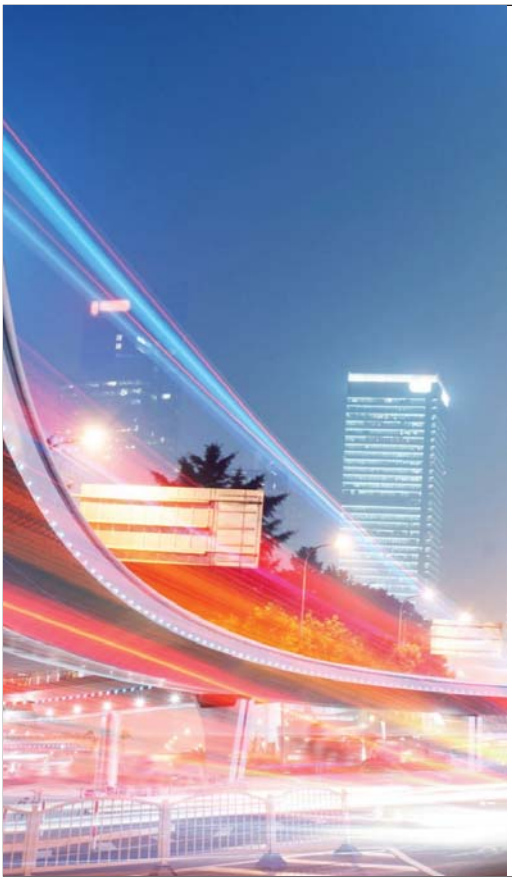
Baker McKenzie.

Canada's Anti-Spam Legislation (CASL) and its Implications for Municipalities

International Municipal Lawyers Association (IMLA)'s 82nd Annual Conference
Niagara Falls, Ontario | October 16, 2017
J. Andrew Sprague, Baker McKenzie





Overview

1. Does CASL apply to municipalities?
2. History of CASL
3. CASL for beginners
4. Private right of action
5. CASL enforcement
6. Parliamentary review
7. Compliance

Disclaimer

This presentation is provided as an information service and is a summary of Canada's anti-spam legislation (CASL). The information in this presentation is not meant as legal advice or opinion, and readers are cautioned not to act on any information provided in this presentation without first seeking specific legal advice with respect to their unique circumstances. The views expressed in this presentation are the personal views of J. Andrew Sprague and, as such, his views do not necessarily reflect the views of Baker & McKenzie LLP or any of its clients.



1 Does CASL apply to municipalities?

Does CASL apply to Municipalities?

- Frequently Asked Questions about Canada's Anti-Spam Legislation

  Question: Does CASL apply to federal, provincial, territorial and municipal governments?

  Answer: CASL does not apply to the activities of the federal, provincial and territorial governments.

  CASL does apply, however, to crown corporations, including municipal governments, when the corporation is acting in the course of any commercial activity.

  http://www.crtc.gc.ca/eng/com500/faq500.htm



2 History of CASL

What does acronym CASL stand for?

- Short Title
  - Unofficially, this Act is called “CASL”, “Canada’s Anti-spam Law” or “Canada’s Anti-spam Legislation” because there is no official short title for this Act.
- Long Title
  - An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23)

2010 to 2017

- Enactment
  - CASL was enacted in 2010
- In Force
  - Many of CASL’s provisions came into force on July 1, 2014.
  - CASL’s provisions relating to computer programs came into force on January 15, 2015.
  - CASL’s private right of action was to come into force on July 1, 2017 – before it was “suspended”.



3 CASL for Beginners

What does CASL regulate?

- CASL regulates a broad range of activities, including:
  - the sending of commercial electronic messages
    - not only emails
    - the definition of “commercial” is very broad
  - the altering of transmission data in an electronic message
  - engaging in fraudulent or misleading practices through electronic messages or websites
  - unsolicited installation of computer programs
  - spyware, malware, botnets, and phishing
  - automated collection of electronic addresses (email harvesting)
  - unlawful use of computers to collection personal information

Important Take-Away

- Under CASL, individuals and organizations are required to have consent in order to be able to do any of the things that are prohibited under the Act, unless they can rely upon a CASL exemption.
  - If anything is to be taken away from this presentation, the importance of consent cannot be over-stated!
  - If an individual or organization does something under CASL that requires consent and they do not have the appropriate consent or they cannot rely upon an exemption, they could be subjected to a number of significant consequences/penalties.

CASL's anti-spam prohibition

- CASL's anti-spam provisions prohibit a sender from transmitting a commercial electronic message ("CEM") to an electronic address, unless:
  i. the intended recipient has consented; and
  ii. the message includes certain prescribed information.

“Electronic Messages”

- “Electronic messages” means a message sent by any means of telecommunication.
  Includes:
  - Text message
  - Sound message
  - Voice message
  - Image message

“Electronic Address”

- “Electronic address” means an address used in connection with the transmission of an electronic message.
  includes, but not limited to:
  - Email
  - Text messaging/SMS
  - Instant messaging
  - Telephone account
  - Social networks (Facebook, LinkedIn)
  - Other online services (web forums, portals)
  - “any similar account”

“Commercial”

- “Commercial” refers to anything that “encourages participation in commercial activity”, including:
  - an offer to purchase, sell, barter or lease a product, goods, a service, land or an interest or right in land
  - an offer to provide a business, investment or gaming opportunity
  - advertising or promotion of these activities or of a person carrying out or intending to carry out these activities

Determining “Commercial”

- In determining if an electronic message is “commercial”, look at:
  - content of the message,
  - the hyperlinks in the message to content on a website or other database, and
  - the contact information contained in the message
- Is it reasonable to conclude, based on the above, that the purpose(s) of the electronic message is to encourage participation in a commercial activity?

“Commercial Activity”

- What is a “commercial activity”?

“any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, **whether or not the person who carries it out does so in the expectation of profit,** ….

High-level Overview

- Four things should be kept in mind:
  - Consents: express or implied
  - Information requirements
  - “Unsubscribe” mechanism requirements
  - Exemptions from consent/information requirements

High-level Overview (continued)

- Remember to keep in mind the following:
  - CEMs can only be sent with a recipient's express or implied consent (unless an exemption applies)
  - Under CASL, the onus of proving sufficient consent rests with the sender of a CEM
  - The recipient of a CEM does not have to prove that he or she did not provide consent
  - An electronic message that requests consent to send a CEM is, under CASL, deemed to be a CEM

How do I understand CASL?

- The *Act*
  - http://laws-lois.justice.gc.ca/eng/acts/E-1.6/index.html

- CRTC's Electronic Commerce Protection Regulations
  - sets out further information as to the form and content of a commercial electronic message (CEM)
  - prescribes detailed requirements when making a request for express consent to send a CEM
  - prescribes requirements relating to computer programs that perform specific functions
  - http://www.crtc.gc.ca/eng/archive/2012/2012-183.htm

How do I understand CASL?

- Industry Canada's Electronic Commerce Protection Regulations
  - defines and clarifies various exemptions under the *Act* (e.g., "family relationship", "personal relationship", "existing business relationship" and "existing non-business relationship")
  - sets out certain classes of commercial electronic messages that are excluded from CASL's requirements
  - prescribes requirements for commercial electronic messages pertaining to referrals

How do I understand CASL?

- Industry Canada's Electronic Commerce Protection Regulations (continued)
  - prescribes requirements where consent is obtained on behalf of a third party
  - defines what "membership" and "club, association or voluntary organization" mean under CASL
  - http://fightspam.gc.ca/eic/site/030.nsf/eng/00273.html

How do I understand CASL?

- CRTC Compliance and Enforcement Information Bulletins
  - Guidelines on the interpretation of the Electronic Commerce Protection Regulations (CRTC) (CRTC 2012-548) (October 10, 2012) (http://www.crtc.gc.ca/eng/archive/2012/2012-548.htm)
  - Guidelines on the use of toggling as a means of obtaining express consent under CASL (CRTC 2012-549) (October 10, 2012) (http://www.crtc.gc.ca/eng/archive/2012/2012-549.htm)
  - Guidelines to help businesses develop corporate compliance programs (CRTC 2014-326) (June 19, 2014) (http://www.crtc.gc.ca/eng/archive/2014/2014-326.htm)

How do I understand CASL?

- Other
  - Guidance on Implied Consent http://www.crtc.gc.ca/eng/com500/guide.htm
  - Requirements for Installing Computer Programs http://crtc.gc.ca/eng/internet/install.htm
  - Enforcement Advisory - Notice for businesses and individuals on how to keep records of consent https://www.canada.ca/en/radio-television-telecommunications/news/2016/07/enforcement-advisory-notice-for-businesses-and-individuals-on-how-to-keep-records-of-consent.html

How do I understand CASL?

- Other (continued)
  - CRTC's website – CASL section
    http://www.crtc.gc.ca/eng/internet/anti.htm
  - CRTC CASL pre-recorded information session
    http://www.crtc.gc.ca/eng/com500/info.htm
  - Frequently Asked Questions
    http://www.crtc.gc.ca/eng/com500/faq500.htm
  - Periodic CRTC update information sessions
    see, for example, "CASL: An Update from the CRTC"
    http://www.cbapd.org/details_en.aspx?id=ON_17OBA0515T

How do I understand CASL?

- Other (continued)
  - Legal community programs
    see, for example, "CASL Challenges Roundtable"
    http://www.cbapd.org/details_en.aspx?id=ON_16PRI0613X
  - Legal community publications
    see, for example, "CASL: A Statistical Analysis from the CRTC"
    http://www.bakerinform.com/home/2017/5/16/canadas-anti-spam-legislation-casl-a-statistical-analysis-from-the-canadian-radio-television-and-telecommunications-commission-crtc,
    https://www.lexology.com/library/detail.aspx?g=e30cbe44-4012-4d10-9970-aba370925eb2, and Canadian Privacy Law Review (July 2017 | Vol. 14, No. 8 | (2017) 14 C.P.L.R.)



4 Private Right of Action

CASL Private Right of Action

- The private right of action under CASL has been repealed – not "suspended"
  - On June 7, 2017, Innovation, Science and Economic Development Canada (formerly known as Industry Canada) announced that on June 2, 2017, the Government of Canada, through an Order in Council, repealed the July 1, 2017 implementation of the private right of action under CASL
  - Widely publicly stated that it has been suspended
  - More information? See http://www.bakerinform.com/home/http/wwwbakermckenziecom/en/people/l/ling-theo-c



5 CASL Enforcement

Why should CASL matter to me?

- CASL applies to all individuals and organizations, unless an exemption is available
- The consequences/penalties under CASL are significant:
  - Administrative Monetary Penalties (AMPs)
    - Up to $1,000,000 per violation for individuals
    - Up to $10,000,000 per violation for any other person (i.e. any legal entity that is not an individual)
  - Corporate officers, directors and agents may be held personally liable for corporate violations
  - Vicarious liability may arise for violations committed by employees or agents
  - Reputational risk and potential public shaming

CASL Enforcement

- Undertakings
  - Plentyoffish Media Inc. (March 2015)
    - $48,000
    - non-compliant unsubscribe
      - mechanism not set out “clearly and prominently”
      - could not be readily performed
    - http://www.crtc.gc.ca/eng/archive/2015/ut150325.htm

CASL Enforcement

- Undertakings
  - Porter Airlines Inc. (June 2015)
    - $150,000
    - non-compliant unsubscribe
      - mechanism not set out “clearly and prominently”
      - mechanism missing
    - missing complete identification information
    - lack of proof of consent
    - http://www.crtc.gc.ca/eng/archive/2015/ut150629.htm

CASL Enforcement

- Undertakings
  - Rogers Media Inc. (November 2015)
    - $200,000
    - non-compliant unsubscribe
      - could not be readily performed
      - unsubscribe from all messages
      - email address for unsubscribe not valid for at least 60 days
      - unsubscribe requests not honoured within 10 business days
    - http://crtc.gc.ca/eng/archive/2015/ut151120.htm

CASL Enforcement

- Undertakings
  - Kellogg Canada Inc. (September 2016)
    - $60,000
    - CEMs sent by Kellogg and/or its third party service providers to recipients without consent
    - http://www.crtc.gc.ca/eng/archive/2016/ut160901.htm

CASL Enforcement

- Undertakings
  - Halazon (June 2017)
    - $10,000
    - non-compliant unsubscribe
      - mechanism did not function
      - could not be readily performed
      - unsubscribe requests not honoured within 10 business days
    - http://www.crtc.gc.ca/eng/archive/2017/ut170612.htm

CASL Enforcement

- Compliance and Enforcement Decision
  - Blackstone Learning Corp. (October 2016)
    - $50,000
    - Nine email campaigns – 385,668 promotional emails sent to employees at 25 Canadian provincial and federal government organizations
    - CEMs sent without consent
    - “conspicuous publication”
    - http://www.crtc.gc.ca/eng/archive/2016/2016-428.htm

CASL Enforcement

- Compliance and Enforcement Decision
  - William Rapanos (March 2017)
    - $15,000
    - 10 violations of section 6
      - non-identification of sender
      - non-inclusion of contact information
      - no prior consent of recipients
      - non-functioning unsubscribe mechanism
    - http://www.crtc.gc.ca/eng/archive/2017/2017-65.htm

CASL Enforcement

- Notice of Violation
  - 3510395 Canada Inc. (Compu-Finder) (March 2015)
    - $1.1 million
    - 3 violations of section 6
      - non-functioning unsubscribe mechanism
      - mechanism not valid for at least 60 days
      - unsubscribe requests not honoured within 10 business days
    - Matter still before the CRTC
    - http://www.crtc.gc.ca/eng/archive/2015/vt150305.htm

CASL Enforcement

- Competition Bureau
  - Aviscar Inc. (Avis) and Budgetcar Inc. / Budgetauto Inc. (Budget) (June 2016)
    - $3 million AMP imposed / $30 million originally sought
    - $250,000 paid towards Bureau's investigative costs
    - False or misleading advertising/representations contained in electronic communications (websites, mobile applications, emails) because advertised prices not attainable due to additional mandatory fees imposed during rental process
    - https://www.canada.ca/en/competition-bureau/news/2016/06/avis-and-budget-to-ensure-prices-advertised-are-accurate.html

CASL Enforcement

- Office of the Privacy Commissioner of Canada (OPC)
  - Compu-Finder
    - e-mail harvesting
    - PIPEDA violations
    - https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-003/
  - http://blog.priv.gc.ca/index.php/2016/05/27/required-reading-for-email-marketers-a-case-study-in-how-not-to-collect-and-use-e-mail-addresses/



6 Parliamentary Review

Parliamentary Review of CASL

- Announced in June 2017
  - https://www.canada.ca/en/innovation-science-economic-development/news/2017/06/government_of_canadasuspendslawsuitprovisioninanti-spamlegislati.html
- Review commenced in September 2017
  - Standing Committee on Industry, Science and Technology (INDU)
  - Statutory Review of CASL http://www.ourcommons.ca/Committees/en/INDU/StudyActivity?studyActivityId=9659639
  - Canadians invited to share their views http://www.ourcommons.ca/DocumentViewer/en/42-1/INDU/news-release/9118472



7 Compliance

Compliance

Due Diligence Defence!

Compliance

- CRTC Guidance
  - Guidelines to help businesses develop corporate compliance programs (CRTC 2014-326) (June 19, 2014) http://www.crtc.gc.ca/eng/archive/2014/2014-326.htm
  - Enforcement Advisory - Notice for businesses and individuals on how to keep records of consent https://www.canada.ca/en/radio-television-telecommunications/news/2016/07/enforcement-advisory-notice-for-businesses-and-individuals-on-how-to-keep-records-of-consent.html
  - Guidance on Implied Consent http://www.crtc.gc.ca/eng/com500/guide.htm

Compliance

- CRTC Guidance on Corporate Compliance
  - Stated purpose is to provide general guidance and best practices on the development of organizational compliance programs to facilitate compliance with CASL as well as the CRTC's Unsolicited Telecommunications Rules (the "Rules").
  - The CRTC acknowledges in the Corporate Compliance Guidelines that no two organizations are the same and every organization has different risks. As a result, compliance programs will vary depending on the size of an organization, its risk profile, and its available resources.

Compliance

- CRTC Guidance on Corporate Compliance
  - Why should an organizational compliance program matter to you and your organization?
  - The Guidelines expressly state the following:

"Commission staff may take into consideration the existence and implementation of an effective corporate compliance program if the business presents the program as part of a due diligence defence in response to an alleged violation of the Rules or CASL. Although the pre-existence of a corporate compliance program may not be sufficient as a complete defence to allegations of violations under the Rules or CASL, a credible and effective documented program may enable a business to demonstrate that it took reasonable steps to avoid contravening the law. Thus, the program may support a claim of due diligence. As well, Commission staff can take the existence of such a program into consideration when determining whether a violation of the Rules or CASL is an isolated incident or is systemic in nature, and whether sanctions against a business should include AMPs [Administrative Monetary Penalties]."

Compliance

- CRTC Guidance on Corporate Compliance
  - Given the potential for serious consequences under CASL (i.e., AMPs of up to $10 million per violation for organizations, personal liability for directors and officers, and vicarious liability for employees' actions), developing, maintaining and updating an organizational compliance program should be on an organization's 'to do' list, especially in light of the CRTC's comments noted on the previous slide.

Compliance

- CRTC Guidance on Corporate Compliance

  - The Guidelines set out the components of an organizational compliance program that the CRTC believes are important. This CRTC does not intend this information to be exhaustive or prescriptive, and organizations may take other reasonable steps to comply with CASL and/or the Rules.

  - The Compliance Guidelines' suggested components of an organizational compliance program are as follows:

Compliance

- CRTC Guidance on Corporate Compliance

  1. Senior Management Involvement

  Senior management of larger organizations should consider playing an active and visible role in fostering a culture of compliance within the whole organization. In addition, thought should be given to giving a member of senior management the responsibility of overseeing the development, management and execution of the organization's compliance program. For smaller organizations, thought should be given to identifying a person who could be responsible for ensuring an organization's compliance.

Compliance

- CRTC Guidance on Corporate Compliance

2. Risk Assessment

The person responsible for overseeing compliance should consider conducting a risk assessment to determine which activities of the organization are at risk for constituting a violation under CASL or the Rules.

Compliance

- CRTC Guidance on Corporate Compliance

3. Written Organizational Compliance Policy

Following the completion of a risk assessment, the person with responsibility should consider developing a written organizational compliance policy. The policy should be made readily accessible to everyone within the organization, kept up-to-date and appropriately reflect how CASL is being interpreted.

Compliance

The Guidelines note that a policy may also:

- establish internal procedures for compliance with the Rules and/or CASL;
- address related training that covers the policy and internal procedures;
- establish auditing and monitoring mechanisms for the corporate compliance program;
- establish procedures for dealing with third parties (for example, partners and subcontractors) to ensure that they comply with the Rules and/or CASL;
- address record keeping, especially with respect to consent; &
- contain a mechanism that enables employees to provide feedback to the chief compliance officer or point person.

Compliance

- CRTC Guidance on Corporate Compliance

4. Record Keeping

The benefits of good record keeping are highlighted in the Guidelines. Of the six benefits listed, the last one may be of great benefit to an organization: “establish a due diligence defence in the event of complaints to the Commission against the business.” It is also suggested that certain records and documents be maintained in hard copy and/or electronic records. The list set out in the Guidelines is worth reviewing.

Compliance

- CRTC Guidance on Corporate Compliance

5. Training Program

Providing training on an organizational compliance program, and providing appropriate follow-up, will be vital to helping an organization ensure that its representatives understand their obligations. In respect of training, the Guidelines go so far as to suggest employees provide, following training, written acknowledgements that they understand the organization's compliance policy. In addition to training, an organization should consider monitoring legislative or regulatory changes, and adjusting their organizational compliance policy, and applicable training, accordingly.

Compliance

- CRTC Guidance on Corporate Compliance

6. Auditing and Monitoring

To help prevent and detect non-compliance, and to assess the effectiveness of the organizational compliance program, an organization should consider performing on-going monitoring and periodic auditing. The results of audits should be recorded, maintained and communicated to the appropriate individuals within an organization, and changes to the organizational compliance policy and program should be made, where appropriate.

Compliance

- CRTC Guidance on Corporate Compliance

7. Complaint-handling System

The Guidelines suggest that organizations put into place a complaint-handling process and that the organization should try to resolve complaints within a reasonable period of time. The CRTC notes that "the complaint-handling system should not be confused with the requirements in the Rules and CASL regarding the withdrawal of consent."

Compliance

- CRTC Guidance on Corporate Compliance

8. Corrective (Disciplinary) Action

The Guidelines suggest that organizations should consider taking corrective or disciplinary action against its representatives to address non-compliance with the organizational compliance policy. Such action may, where appropriate, include refresher training.

Compliance

- Resources Provided
  - Sample Electronic Communications Survey
  - Sample Compliance Preparedness Checklist
  - Baker McKenzie Client Alert titled "*Canada's Anti-Spam Law To Come Into Force July 1, 2014*" (December 2013)
  - Baker McKenzie "CASL" article published in Getting the Deal Through (2015)
  - Thomson Reuters – Practical Law – Direct Marketing Country Questions for Canada (December 2016), written by Baker McKenzie

Niagara Falls, Ontario, Canada

National Service Dog (NSD) Flicka hopes that you've enjoyed Niagara Falls.











Questions or Comments?

J. Andrew Sprague
Professional Support Lawyer
Baker & McKenzie LLP

T: +1 416 865 2344
E: Andrew.Sprague@BakerMcKenzie.com



https://www.linkedin.com/in/asprague/
https://twitter.com/jandrewsprague
http://www.bakermckenzie.com/en/people/s/sprague-j-andrew

Client Alert

December 2013

Canada's Anti-Spam Law To Come Into Force July 1, 2014

Introduction

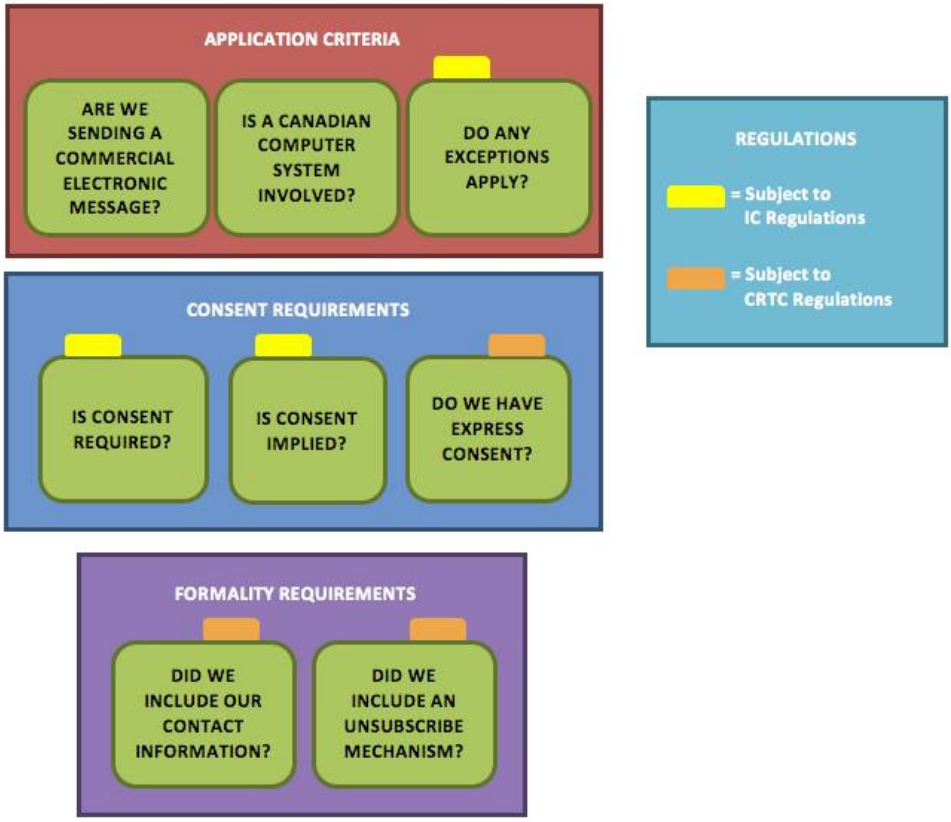
Email and other forms of electronic communication have become an integral part of the modern economy – and an indispensable tool in organizations' business operations, relationships, marketing campaigns and other commercial activities. Electronic spam, however, can be associated with harms ranging from unwanted emails and other electronic communications to malware, viruses and fraud. To address these harms, the Canadian government passed sweeping legislation in 2010 that has become known as Canada's Anti-Spam Legislation (CASL). After a considerable delay, which involved multiple public consultations and several rounds of draft regulations, the government announced in early December that most aspects of CASL will finally come into force on **July 1, 2014**.

By most accounts, CASL imposes onerous requirements with respect to the transmission of commercial electronic communications. Penalties for non-compliance run as high as **$10 million CAD** in potential administrative monetary penalties for organizations. Moreover, starting on July 1, 2017, a private right of action for non-compliance with CASL will become available, exposing organizations to the risk of class actions. Parties found to have sent non-compliant electronic messages could be subject to statutory damages of $200 per contravention to a maximum of **$1 million per day**, in addition to compensatory damages. It is critical that organizations use the next six months to ensure compliance with CASL.

This alert is intended to guide you through a high-level summary of the main compliance issues that you will need to consider when sending commercial electronic communications, based on CASL and the two sets of regulations registered under it by Industry Canada (the "IC Regulations") and the Canadian Radio-television Telecommunications Commission (the "CRTC Regulations"). However, the requirements of CASL are detailed and complex. They will be subject to both existing and forthcoming government interpretation guidelines and FAQs. Every organization will need to consider its compliance obligations in light of its own activities and circumstances.

Summary of the Law

The Main Issues related to the Transmission of Commercial Electronic Messages



Application Criteria

Are we sending a commercial electronic message?

CASL generally prohibits parties from sending a “commercial electronic message” to a recipient who has not expressly consented to receiving it and unless it complies with prescribed formality requirements such as including the sender’s mailing address and an unsubscribe mechanism. To determine whether CASL applies to your communication, you must first determine whether it is an electronic message, which is defined broadly to include email, text messages, social media communications, and any other message sent by telecommunication. If it is an electronic message, you must determine if it is commercial, meaning that one would reasonably conclude that the message has as one of its purposes the encouragement of participation in a commercial activity. A commercial activity is defined to include activities whether or not carried out with an expectation of profit.

Is a Canadian computer system involved?

If you are sending a commercial electronic message, then CASL will apply to you if a computer system located in Canada is used to send or access the message, subject to exceptions provided in the legislation or regulations. Certain provisions of CASL will also apply where such a computer system is used in routing the message.

Do any exceptions apply?

There are circumstances where neither the express consent nor the formality requirements of CASL apply to the transmission of commercial electronic messages. For instance, CASL provides that these requirements do not apply to commercial electronic messages between parties in a **personal** or **family relationship** according to specific criteria. Recently finalized IC Regulations now also include other specific exceptions relevant to businesses and other organizations, including in particular:

- **Organization-to-organization communications**: Communications sent within an organization or between organizations that have a relationship, and the message concerns the activities of the organization to which the message is sent.

- **Solicited communications**: The message is sent in response to a request, inquiry or complaint.

- **Legal communications**: The message involves enforcing or satisfying a right, legal or juridical obligation, court order, judgment or tariff.

- **Limited access accounts**: The message is sent to a "limited-access secure and confidential account" provided by the sender to the recipient, and the sender is the only one able to send messages to that account. This exception is expected to apply to systems in which users create an online account with an organization for a limited purpose, such as an online banking account.

- **Electronic messaging service**: The commercial electronic message is sent and received on an "electronic messaging service" where the formality requirements are satisfied through the service's user interface, and the person has consented either expressly or by implication. This exception appears to be intended to encompass messages sent within common social media platforms and similar systems.

- **Foreign recipients**: The message is sent to a recipient in a jurisdiction outside Canada with its own anti-spam legislation that is listed in a schedule to the IC Regulations and the message conforms with the anti-spam law of that jurisdiction.

- **Charities**: The message is sent by or on behalf of a Canadian registered charity and the message has as its primary purpose raising funds for the charity.

- **Political parties**: The message is sent by or on behalf of a Canadian political party, organization or candidate and the message has as its primary purpose soliciting political contributions.

Consent Requirements

Is consent required?

If CASL applies to your commercial electronic message, you must determine if you are required to obtain the recipient's consent to receiving the message. CASL outlines a number of circumstances in which the addressee's consent is not required, mainly because the message contains information that the addressee is

already expecting or entitled to receive. For example, if a person has purchased a product from you, then you do not need the addressee's consent to send him or her product recall information about that product. If your compliance with CASL is challenged, you bear the onus of proving that you obtained valid consent in all applicable circumstances.

The IC Regulations also establish an exception to the consent – but not the formality – requirement in referral situations, where the commercial electronic message was sent to a recipient who was referred to the sender by a mutual contact, the message discloses the full name of the mutual contact and the message states that it is being sent as a result of the referral. This exception only applies to the first message sent as a result of such a referral, and specific requirements must be met for a party to be considered a mutual contact. However, it would permit a first message to be sent without consent in some cases.

Is consent implied?

If consent is required, CASL provides circumstances in which an individual gives implied consent to receive commercial electronic messages from the sender. For example, consent is implied where the sender and recipient have **an existing business relationship**, which is generally defined to mean that the sender and recipient have entered a purchase or lease transaction over the past two years or corresponded with respect to a potential transaction over the past six months, subject to transitional provisions. These requirements will impose duties on businesses and other organizations to scrutinize their databases for when an individual recipient last gave implied consent and to keep track of how long it will be before such consent expires.

Consent is also implied where the parties have **an existing non-business relationship**. CASL provides several circumstances in which such a relationship exists, including where the recipient of an electronic message is or was a member of the sending organization within the past two years, subject to transitional provisions, and the sending organization is a club, association or voluntary organization as defined in regulations.

However, CASL generally limits the circumstances in which consent is implied to specifically listed categories. Importantly, consent obtained under privacy laws may not be sufficient consent for purposes of implied consent under CASL.

Do we have express consent?

If consent is not implied and no other relevant exceptions apply, then you must obtain an individual’s express consent before you are permitted to send him or her a commercial electronic message. The CRTC Regulations help to clarify what information must be included in a request for consent. In particular, you must set out simply and clearly the name of your business or organization, your mailing address and either your phone number, email address or web address, and a statement indicating that you intend to send the individual commercial electronic messages and that he or she can withdraw his or her consent. Guidelines issued by the CRTC state that express consent is obtained through opt-in mechanisms, such as checking a box or typing in an email address.

Formality Requirements

Did we include our contact information?

Unless an exception applies, you must include certain contact information in commercial electronic messages such as the name of your business or organization, your mailing address and either your phone number, email address or a web address. The CRTC Regulations provide that such information may be posted on a readily accessible webpage if it is impracticable to include it in the message itself.

Did we include an unsubscribe mechanism?

Commercial electronic messages must contain a clear and prominent unsubscribe mechanism at no cost to recipients and which uses the same electronic means by which the message was sent, or if impracticable, another electronic means. The unsubscribe mechanism must also include an electronic or web address to which a recipient may send his or her request not to be sent any further commercial electronic messages. The sender must ensure that this address is valid for a minimum of 60 days after the message has been sent and that an unsubscribe request must be given effect within 10 business days. The CRTC Regulations provide that the unsubscribe mechanism may be posted on a readily accessible webpage if it is impracticable to include it in the message itself.

What to Do Before CASL Takes Effect

CASL will impose numerous requirements with respect to the transmission of commercial electronic messages that must be in place prior to **July 1, 2014**.

To meet this timeline, you will likely need to take some of the following steps over the next six months, if you have not done so already:

- Determine which of your electronic communications, including commercial and promotional emails, social media communications and text message alerts, would qualify as commercial electronic messages;
- Establish a system that allows you to record and manage express consents and monitor how long it has been since they were obtained;
- Prepare a compliant unsubscribe mechanism to accompany all commercial electronic messages;
- Establish a procedure that ensures that parties that have unsubscribed to your messages or otherwise indicated their request not to receive any more messages will not be sent messages in the future;
- Identify which exceptions to the consent and formality requirements may apply to your commercial electronic messages;
- If you rely on any implied consents, establish a system that allows you to record and monitor the status of your relationships with other parties, such as a tickler system that ensures that an existing business relationship continues to exist;

- Prepare a compliant opt-in mechanism that customers can use to receive promotional messages;

- Ensure that all necessary contact information accompanies your commercial electronic messages;

- Make any necessary internal IT infrastructure investments and upgrades to effect these requirements, and approach marketing and other external service providers to ensure they will be able to support activities they undertake on your behalf in full compliance with CASL after July 1, 2014.

CASL also contains other important restrictions relevant to commercial electronic messages, including prohibiting without express consent the alteration of message transmission data or the rerouting of messages to a different destination than authorized; expressly prohibiting the unauthorized harvesting of email addresses; and expanding existing civil and criminal laws prohibiting false or misleading representations to include specifically those in electronic communications, including in text, email headers, sender information, subject lines and URLs.

In addition to these requirements, CASL will impose express consent, notice and other requirements related to the installation of computer programs on the computer systems of others in the course of a commercial activity, which will take effect in January 2015 and may apply if you distribute software electronically or use software to interact with customers and business partners.

If you have business activities in multiple jurisdictions, you will need to consider how certain requirements of CASL may differ from your existing legal obligations under anti-spam laws in other jurisdictions.

Once it takes effect, CASL will be among the most restrictive and onerous anti-spam legislation globally and create significant new risk for companies that are not compliant.

Additional Links to Government Materials

CASL, as adopted in December 2010, is available at
http://laws-lois.justice.gc.ca/eng/acts/E-1.6/index.html

The final CRTC Regulations are available at
http://laws-lois.justice.gc.ca/eng/regulations/SOR-2012-36/index.html

The final IC Regulations are available at
http://fightspam.gc.ca/eic/site/030.nsf/eng/00273.html

Industry Canada's Regulatory Impact Analysis Statement is available at
http://fightspam.gc.ca/eic/site/030.nsf/eng/00271.html

A press release is available at http://news.gc.ca/web/article-eng.do?nid=798829

A backgrounder is available at http://www.ic.gc.ca/eic/site/064.nsf/eng/07401.html

www.bakermckenzie.com

For further information please contact

Theodore Ling
+1 416 865-6954
Theodore.Ling@bakermckenzie.com

Arlan Gates
+1 416 865-6978
Arlan.Gates@bakermckenzie.com

Lisa Douglas
+1 416 865-6972
Lisa.Douglas@bakermckenzie.com

Eva Warden
+1 416 865-2350
Eva.Warden@bakermckenzie.com

Jonathan Tam
+1 416 865-2324
Jonathan.Tam@bakermckenzie.com

Baker & McKenzie LLP
Barristers & Solicitors
Brookfield Place
Bay/Wellington Tower
181 Bay Street, Suite 2100
Toronto, Ontario M5J 2T3
Canada

©2013 Baker & McKenzie. All rights reserved. Baker & McKenzie International is a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.

This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Canada's Anti-Spam Law

Theo Ling, Arlan Gates, Lisa Douglas, Eva Warden and Jonathan Tam
Baker & McKenzie LLP

Introduction

Through its wide scope of application, rigorous standards, and potential imposition of steep financial penalties, Canada's Anti-Spam Law (CASL) has created an imperative for businesses and other organisations to ensure conformity with the new legislation. At the same time, the law's complex assortment of exemptions, its flexibly worded definitions, multiple regulations, guidelines and interpretations, and its intended purpose of deterring the most egregious forms of unsolicited electronic communications, call for a nuanced consideration of whether and how an organisation should revise its practices and programs for compliance purposes.

The core provisions of CASL, which came into force on 1 July 2014, generally prohibit the sending of a commercial electronic message (CEM) without the recipient's explicit consent and unless the message complies with certain formality requirements such as including the sender's contact information and an unsubscribe mechanism. The law applies broadly to anyone who sends, or causes or permits the sending of, a CEM, and its extraterritorial reach extends to any circumstance where a computer system located in Canada is used either to send or to access the message, with limited exceptions.

Starting on 15 January 2015, CASL will also generally prohibit the installation of computer programs on another person's computer system in the course of a commercial activity, unless express consent has been obtained in accordance with prescribed disclosure requirements. In the case of computer programs that perform certain functions, such as collecting personal information stored on the computer system or changing previously installed settings, additional disclosure, consent and service requirements will apply.

The Canadian Radio-television and Telecommunications Commission (CRTC) will have primary responsibility for enforcing CASL, in collaboration with the Canadian Competition Bureau and Office of the Privacy Commissioner. Failure to comply with CASL could result in civil administrative monetary penalties of up to C$10 million per violation. Moreover, starting on 1 July 2017, a private right of action for non-compliance with CASL will become available, exposing organisations to the risk of class actions. Parties found to have sent CEMs or installed computer programs in violation of CASL could then be subject to statutory damages of $1 million per day on which a contravention occurred, in addition to compensatory damages.

The following is a high-level summary of the main requirements relating to the sending of CEMs and the installation of computer programs under CASL. However, the law's detailed and complex requirements will be subject to both existing and forthcoming government interpretation guidelines, bulletins and enforcement experience. Every organisation will be affected differently and must consider its compliance obligations in the context of its own activities and circumstances.

Sending electronic messages

Application criteria

Is a commercial electronic message being sent to an electronic address?

CASL generally prohibits sending a commercial electronic message to an electronic address unless certain criteria are met. The prohibition and criteria do not apply to messages that are not commercial electronic messages as defined in the statute.

CASL defines electronic messages broadly to include any message sent by any means of telecommunication including a message containing text, sound, voice or image.

An electronic message is a CEM under CASL if it would be reasonable to conclude that it has as one of its purposes (not necessarily the primary purpose) to encourage participation in a commercial activity. A commercial activity is in turn defined to mean activities of a commercial character, whether or not carried out with an expectation of profit.

Further, CASL only applies if the CEM is being sent to an electronic address, which is defined to include an email, instant messaging, telephone or other similar account. CASL's prohibition on the transmission of commercial electronic messages therefore does not apply to website banner advertisements or social media posts and similar publications that are not sent to individual electronic addresses. Two-way telephone calls, broadcast voicemails and fax messages are also excluded.

Is a computer system located in Canada involved?

The requirements of CASL relating to the transmission of CEMs apply only if a computer system that is located in Canada is used to send or access the electronic message.

Do any exemptions apply?

CASL establishes a number of complete exemptions to both the consent and the formality requirements for the transmission of CEMs. These exemptions include the following:

- *Personal relationship*: The sender and recipient are individuals in a personal relationship, meaning that they have had direct, voluntary, two-way communication and that it be reasonable to conclude that they are in a personal relationship. A very narrow exemption for certain family relationships is also available.
- *Internal communications within an organisation*: An employee, representative, consultant or franchisee of an organisation sends a message to another employee, representative, consultant or franchisee of the same organisation and the message concerns the activities of the organisation.
- *Organisation-to-organisation communications*: One employee, representative, consultant or franchisee of an organisation sends a message to an employee, representative, consultant or franchisee of another organisation, if the organisations have a 'relationship' and the message concerns the activities of the receiving organisation.
- *Solicited communications*: The message responds to a request, inquiry or complaint or was in some other way solicited by the recipient.
- *Legal communications*: The message consists of enforcing or satisfying a right, legal or juridical obligation, court order, judgment or tariff.
- *Limited access accounts*: The message is sent to a secure, confidential and limited-access account provided by the sender, and the sender is the only one able to send messages to the recipient using that account.
- *Foreign recipients*: The sender reasonably believes that the message will be received in a jurisdiction outside Canada that is listed in a schedule under CASL, and the message complies with the anti-spam law of that jurisdiction.
- *Charities*: The message is sent by or on behalf of a Canadian registered charity and the primary purpose of the message is raising funds for the charity.

- *Political parties*: The message is sent by or on behalf of a Canadian political party, organisation or candidate and the primary purpose of the message is soliciting political contributions.
- *Electronic messaging services*: The message is sent and received on an electronic messaging service if the sender identification and unsubscribe mechanism are conspicuously published and readily available on the user interface and the person to whom the message was sent expressly or implicitly consented.

Consent requirements

Is consent required?

CASL provides a number of limited exemptions from the requirement to obtain consent, but not from the formality requirements applicable to CEMs. These exemptions apply in certain circumstances where the message contains information that the addressee is already expecting or entitled to receive.

For example, CASL does not require consent to send a message that provides warranty information, product recall, or safety or security information about a product purchased by the recipient. However, these exceptions are only available if the message *solely* contains the kind of information permitted by the exception. Thus, the exception for product recall information does not apply if the message also includes non-exempt content such as information about a product or a promotion.

CASL also contains a limited exception to the consent requirements in certain referral situations, and creates special rules for obtaining consent on behalf of an unknown third party, as in the case of a list provider.

Is consent implied?

CASL provides that consent, if required, may be implied in some circumstances, which are limited to the following:

- *Existing business relationship*: the sender and recipient have entered into a purchase or lease transaction, or certain other types of transactions, over the past two years or the recipient has made a commercial inquiry over the past six months, subject to transitional provisions.
- *Existing non-business relationship*: the recipient is or was a member of the sending organisation within the past two years, subject to transitional provisions, and the sending organisation is a club, association or voluntary organisation as defined in CASL.
- *Conspicuous publication or disclosure of electronic address*: the recipient has conspicuously published or disclosed to the sender his or her electronic address, without indicating that he or she does not wish to receive unsolicited commercial electronic messages, and the message relates to his or her functions in a business or official capacity.

CASL provides that where there was an existing business relationship or existing non-business relationship before 1 July 2014 (the coming into force date) that involved the sending of CEMs, consent can be implied for three years after that date; otherwise, the limitation periods noted above apply. There are no time limitations on implied consent based on conspicuous publication or disclosure, under the transitional provision or otherwise.

Has express consent been obtained?

If consent is not implied and no other exceptions apply, the sender must obtain a person's express consent before sending him or her a CEM.

CASL requires disclosure of certain pieces of information when requesting a person's express consent. In particular, the person requesting consent must set out simply and clearly the name of its business or organisation, its mailing address and either its phone number, email address or web address, and a statement indicating that the prospective recipient can withdraw his or her consent to receive CEMs at any time. Express consent must be sought separately from any other request and must be obtained through opt-in mechanisms, such as checking a box, typing in an email address, or responding affirmatively to an oral question specifically about receiving CEMs.

Importantly, consent received under Canada's federal private sector privacy legislation, PIPEDA, may not be sufficient for the purposes of CASL. PIPEDA generally requires an individual's informed consent, but not necessarily express consent, before using his or her personal information in any way. Disclosing information practices in a privacy policy or terms of service will not be sufficient under CASL. However, express consent obtained in compliance with PIPEDA before 1 July 2014 will be recognised as compliant, whether or not it was obtained according to the specific disclosure and other requirements for opt-in consent under CASL.

Formality requirements

Does the CEM include the sender's contact information?

Unless an exception applies, CEMs must disclose certain contact information including the sender's business name, the sender's mailing address, and one of the sender's e-mail address, telephone number or web address. Such information may be posted on a readily accessible webpage if it is impracticable to include it in the message itself. The contact information must be accurate and valid for at least 60 days after the sending of the CEM.

Does the CEM include an unsubscribe mechanism?

CASL also generally requires that CEMs contain a clear and prominent, 'readily performed' unsubscribe mechanism at no cost to recipients and which uses the same electronic means by which the message was sent, or if impracticable, another electronic means. The sender must ensure that an unsubscribe request be given effect within 10 business days. The unsubscribe mechanism may be posted on a readily accessible webpage if it is impracticable to include it in the message itself.

Steps to ensure compliance

Businesses and other organisations may need to review and, in some cases, adjust their current practices for compliance with CASL's requirements for sending CEMs. Measures to ensure compliance may include:

- an assessment of the organisation's electronic communications to identify those that would qualify as CEMs and, if so, whether any exemptions are likely to apply;
- the inclusion of required sender identification and implementation of a functioning unsubscribe mechanism in outgoing CEMs; and
- the implementation of an opt-in mechanism to obtain express consent from prospective recipients of CEMs where required.

The CRTC has also recommended the development of corporate compliance programs that include senior management involvement, risk assessments, a written policy, record-keeping and auditing, effective staff training, a complaint-handling system, and corrective/disciplinary action to address contraventions.

Such measures can help organisations ensure compliance with CASL, and bring them within the law's due diligence defence, which permits a person alleged to be in violation of the statute to argue that it took reasonable steps to avoid the violation.

Installing computer programs

Application criteria

Does the prohibition apply to the conduct in question?

CASL generally prohibits installing a computer program on another person's computer system in the course of a commercial activity unless that person's express consent has been obtained.

Although the term 'install' is not defined within CASL, a 'computer program' is broadly defined as data representing instructions or statements that cause a computer system to perform a function when executed.

The requirements around the installation of computer programs may apply, among other scenarios, to the distribution of apps, computer programs, or other software electronically, or use of software to interact with customers and business partners.

Is the computer system or the person installing the program located in Canada?

CASL's requirements for the installation of computer programs apply if the computer system on which the program is installed is located in Canada. Alternatively, the requirements apply if the person installing the program is in Canada or is acting under the direction of a person who is in Canada.

General requirements

Is express consent deemed?

A person is considered to expressly consent to the installation of certain types of programs, including the following:

- a cookie;
- HTML code;
- Java Scripts (an undefined term that likely covers JavaScript that is executed in a browser; it is unclear whether it would apply to Java applets that download and run in a browser but are executed outside the browser);

- an operating system;
- a program that is executable only through the use of a computer program whose installation or use the person has previously expressly consented to; and
- a program that is necessary to correct a failure in the operation of the computer system (or a computer program installed on the computer system), and which is installed solely for that purpose.

Special exemptions are also available for computer programs installed by or on behalf of telecommunications service providers.

Has express consent been obtained?

Unless an exception applies, and subject to the special requirements outlined below, a person's express consent is required to install a computer program on his or her computer system in the course of a commercial activity. Certain disclosures must be made when requesting that person's express consent.

In particular, the request must provide a clear and simple description, in general terms, of the function and purpose of the computer program that is to be installed on the person's computer system. The request must also disclose the same types of information that must be disclosed when requesting express consent to send a CEM, such as prescribed contact information and a statement indicating that the person can withdraw his or her consent.

In general, once a person's express consent has been obtained, the above information does not need to be restated when requesting the person's consent to install an upgrade or update to that computer program. However, this exception only applies if the person is entitled to receive the update or upgrade, and it is installed in accordance with the terms of the express consent of the original computer program's installation.

Special requirements

Does the computer program perform any unexpected functions?

CASL imposes special disclosure, consent and service requirements for the installation of computer programs that will cause the computer system to operate in a manner contrary to the reasonable expectations of the owner or an authorised user of the computer system. These requirements, which are intended to deter unauthorised installation of malicious computer programs, apply to the following prescribed functions:

- collecting personal information stored on the computer system;
- interfering with the user or authorised user's control of the computer system;
- changing or interfering with settings, preferences or commands already installed or stored on the computer system without the knowledge of the owner or authorised user;
- changing or interfering with data that is stored on the computer system in a manner that interferes with the owner or authorised user's lawful access to or use of that data;
- causing the computer system to communicate with another computer system without the authorisation of the owner or authorised user; and
- installing a computer program that may be activated by a third party without his or her knowledge.

Special disclosure requirements

Unless a specific exception applies, a request for consent to install a computer program that performs one of the abovementioned functions must describe, clearly and prominently, the computer program's material elements that perform such functions, including the nature and purpose of those elements and their reasonably foreseeable impact on the operation of the computer system. These material elements must be brought to the attention of the owner or authorised user of the computer system separately from the licence agreement and any other information provided in the request for consent. The general requirements for obtaining express consent to install a computer program also apply.

Special consent requirements

In order to be valid under CASL, express consent to install a computer program that performs any of the above-mentioned functions must be sought separately from any other request for consent. Further, the person seeking consent must obtain an acknowledgment in writing from the owner or authorised user that he or she understands and agrees that the computer program performs such functions. The term 'in writing' includes both paper and electronic forms of writing, so long as it can subsequently be verified.

Special service requirements

For a period of one year after the installation of a computer program that performs any of the abovementioned functions, and unless a specific exception applies, the person who gave consent must be provided with an electronic address to which he or she may send a request to remove or disable the computer program if he or she believes that the function, purpose or impact of the computer program installed was not accurately described in the request for consent. Upon receipt of such a request within the one-year period, if the request is not without merit, the person who has the owner or authorised user's express consent must assist in removing or disabling the program as soon as feasible without cost to him or her.

Steps to ensure compliance by 15 January 2015

Measures to ensure an organisation's compliance with the provisions relating to installation of computer programs may include:

- an assessment of the organisation's activities to identify those that involve the installation of computer programs in the manner covered by CASL, and, if so, whether any exceptions are likely to apply;
- preparation of a clear and simple summary of the programs' functions and purposes to accompany requests for express consent, along with the other basic disclosure requirements;

BAKER & McKENZIE

Theo Ling **theo.ling@bakermckenzie.com**
Arlan Gates **arlan.gates@bakermckenzie.com**
Lisa Douglas **lisa.douglas@bakermckenzie.com**
Eva Warden **eva.warden@bakermckenzie.com**
Jonathan Tam **jonathan.tam@bakermckenzie.com**

181 Bay Street, Suite 2100
PO Box 874, Brookfield Place
Toronto, Ontario M5J 2T3
Canada

Tel: +1 416 863 1221
Fax: +1 416 863 6275
www.bakermckenzie.com

- identification of any computer programs that perform any of the prescribed functions that will cause the computer system to operate in a manner contrary to the owner or authorised user's reasonable expectations; and
- for programs that perform such functions, implementation of a means of obtaining the user's separate and informed consent, in accordance with the special requirements under CASL, as well as a means of responding to reasonable requests in the year following installation to remove or disable the program.

The core provisions of CASL are now in effect. However, a phased-in approach to CASL's coming into force, including a three-year transitional period during which organisations can rely on implied consent to send CEMs where there is an existing relationship that pre-dates 1 July 2014, the delayed effective dates of provisions relating to the installation of computer programs, the private right of action and indications that the CRTC will take a reasonable case-by-case approach to alleged violations afford organisations an ongoing opportunity to assess their internal information structure and practices and develop tailored solutions to meet CASL obligations.

THOMSON REUTERS
PRACTICAL LAW™

DIRECT MARKETING COUNTRY QUESTIONS: **CANADA**

This document is published by Practical Law and can be found at: **www.practicallaw.com/4-636-9037**
Request a free trial and demonstration at: **www.practicallaw.com/about/freetrial**

Canada specific information concerning direct marketing laws.

This Q&A provides country-specific commentary on *Direct marketing: international overview*, and forms part of our *Sales and Marketing International Transaction Guide*.

Arlan W. Gates and J. Andrew Sprague, Baker & McKenzie LLP

RESOURCE INFORMATION

RESOURCE ID

4-636-9037

RESOURCE TYPE

Country Q&A

STATUS

Law stated as at 01-Dec-2016

JURISDICTION

Canada

THE REGULATION OF UNSOLICITED COMMERCIAL COMMUNICATIONS

1. How does national law regulate the making of unsolicited telephone calls for marketing purposes?

Under section 41(1) of the federal Telecommunications Act (*S.C. 1993, c. 38, as amended*), the Canadian Radio-television and Telecommunications Commission (CRTC) "may, by order, prohibit or regulate the use by any person of the telecommunications facilities of a Canadian carrier for the provision of unsolicited telecommunications to the extent that the Commission considers it necessary to prevent undue inconvenience or nuisance, giving due regard to freedom of expression."

The CRTC regulates the making of unsolicited telephone calls for marketing purposes through the Unsolicited Telecommunications Rules (UTRs). The UTRs were first established in 2007 (*Telecom Decision 2007-48*) and have been amended a number of times since.

All parts of the UTRs apply to unsolicited communications to individuals, and some parts of the UTRs apply to unsolicited communications to companies.

NATIONAL DO NOT CALL LIST (DNCL) RULES

A national do not call list (the National DNCL) was established under the Telecommunications Act in 2007, and the National DNCL Rules were implemented.

The National DNCL Rules are set out in Part II of the UTRs. The rules do not apply to telemarketing telecommunications made to a business consumer. In addition, they do not apply in respect of telecommunications made:

- By or on behalf of a registered charity.
- To a person:
  - with whom the person making the telecommunication, or the person or organisation on whose behalf the telecommunication is made, has an existing business relationship; and
  - who has not made a do not call request in respect of the person or organisation on whose behalf the telecommunication is made.
- By or on behalf of a registered political party.
- By or on behalf of a nomination contestant, leadership contestant or candidate of a registered political party, or by or on behalf of the official campaign of such contestant or candidate.
- By or on behalf of an association of members of a registered political party for an electoral district.
- For the sole purpose of collecting information for a survey of members of the public.
- For the sole purpose of soliciting a subscription for a newspaper of general circulation.

Under the National DNCL Rules, a telemarketer is not permitted to initiate a telemarketing call:

- To a consumer's telephone number that is on the National DNCL, unless the consumer has provided express consent to the telemarketer to be contacted via telemarketing telecommunication.
- On its own behalf unless it is a registered subscriber of the National DNCL and it has paid all applicable fees to the National DNCL operator.
- On behalf of a client unless the client is a registered subscriber of the National DNCL and the applicable fees to the National DNCL operator associated with the client's subscription have been paid.

The National DNCL Rules set out record keeping requirements with which telemarketers must comply, and specific obligations and restrictions imposed on telemarketers and their clients in respect of the National DNCL.

Reproduced from Practical Law, with the permission of the publishers. For further information visit practicallaw.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2016. All Rights Reserved.

THOMSON REUTERS®

TELEMARKETING RULES

The Telemarketing Rules are set out in Part III of the UTRs. They apply irrespective of whether the telemarketing telecommunication is exempt from the National DNCL Rules, and therefore apply to unsolicited communications both to individuals and to companies.

The Telemarketing Rules do not apply to:

- Telemarketing telecommunications made via voice mail broadcast (that is, a telecommunication where a recorded message is delivered directly into a person's voice mailbox without interrupting that person's activities in real time).
- Unsolicited telecommunications made for purposes other than solicitation, including telecommunications made solely for the purpose of emergencies, account collection, collecting information for a survey of members of the public, and market research.

Under the Telemarketing Rules, a telemarketer may not initiate an unsolicited telemarketing call:

- On its own behalf unless it has registered with, and provided information to, the National DNCL operator, and it has paid all applicable fees charged by the CRTC's Complaints Investigator delegate.
- On behalf of a client unless the client has registered with and provided information to the National DNCL operator, and all applicable fees charged by the CRTC's Complaints Investigator delegate associated with the client have been paid.

The Telemarketing Rules set out obligations and restrictions imposed on telemarketers and their clients, including record keeping requirements.

For example, subject to more restrictive requirements set out in provincial legislation, consumers may only receive telemarketing telecommunications during the following hours and days:

- 9.00 am to 9.30 pm on weekdays (Monday to Friday).
- 10.00 am to 6.00 pm on weekends (Saturday and Sunday).

Sequential dialling for the purpose of initiating a telemarketing telecommunication is prohibited under the Telemarketing Rules, and telemarketing telecommunications to healthcare facilities are prohibited. In addition, the Telemarketing Rules contain in-call disclosure requirements.

ADAD RULES

Automatic dialling-announcing devices (ADADs) are subject to additional rules (the ADAD Rules), set out in Part IV of the UTRs.

The ADAD Rules set out specific obligations and restrictions regarding ADADs. The rules apply irrespective of whether the telemarketing telecommunication is exempt from the National DNCL Rules, and therefore cover both calls to individuals and to companies.

2. How does national law regulate direct marketing by fax?

The Telemarketing Rules also apply to direct marketing by fax (see *Question 1*).

In addition to numerous other obligations and restrictions set out in the Telemarketing Rules, when a telemarketer sends a fax telemarketing communication, specific information must be clearly disclosed at the top of the first page in font size 12 or larger.

The Telemarketing Rules apply irrespective of whether the telemarketing telecommunication is exempt from the National DNCL Rules, and therefore cover unsolicited communications both to individuals and to companies.

3. How does national law regulate direct mail advertising?

Direct mail advertising is not specifically regulated by national law, in contrast to other forms of direct marketing (for example, unsolicited telephone calls, faxes and emails).

Canada's national mail carrier is Canada Post. Direct mail advertising delivered by Canada Post is subject to requirements and restrictions under the Canada Post Corporation Act (*R.S.C. , 1985, c. C-10*) and regulations and Canada Post guidelines.

In general, Canada Post will consider non-mailable any direct mail that includes:

- Illegal, obscene or fraudulent materials.
- Dangerous articles or substances.
- Sexually explicit materials (unless properly packaged).
- Modified postage stamps or Canada Post marks.
- Mail that fails to meet physical characteristics and marking requirements set out in guidelines.

Under the Solicitations by Mail Regulations made under the Canada Post Corporation Act, solicitations sent by email that appear to be a bill, invoice, or account statement but do not in fact require payment unless an offer is being accepted must comply with prescribed wording and formatting requirements..

4. How does national law regulate direct marketing by e-mail?

Canada's national law regulating direct marketing by email is known as Canada's Anti-Spam Legislation or

Reproduced from Practical Law, with the permission of the publishers. For further information visit practicallaw.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2016. All Rights Reserved.

CASL. CASL's official name is "An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act" (*S.C. 2010, c. 23*).

To send a commercial electronic message (CEM) to a recipient, the sender must have the express consent of the intended recipient, and the sender's CEM must include specific prescribed information, unless the sender can rely on an exemption or implied consent under CASL.

The definition of a CEM under CASL is very broad and includes electronic messages such as email, text messaging/SMS, instant messaging, certain activity on social networks (Facebook, LinkedIn, and so on), and other online services (for example, web forums and portals).

CASL defines a CEM as an electronic communication whose purpose is, among others, to encourage participation in a commercial activity. This includes a transaction, or any conduct of a commercial character, whether or not it is carried out with the expectation of profit. This would therefore encompass CEMs offering, advertising or promoting a product or service, or promoting the public image of a person engaged in such sales, advertising or promotion.

In determining whether an electronic message is "commercial", the CRTC will look at:

- The content of a message.
- The hyperlinks in a message to content on a website or other database.
- The contact information contained in the message.

The test applied is whether it is reasonable to conclude, based on the factors above, that one or more of the purposes of an electronic message is to encourage participation in a commercial activity.

CONSENT

Consent to send a CEM may be either express or implied. Under CASL, the burden of proving sufficient consent rests with the sender. The CRTC issued an Enforcement Advisory in July 2016 to remind organisations of this obligation. An electronic message requesting consent to send a CEM is also considered a CEM under CASL, and cannot be sent without existing express or implied consent.

Requests for express consent must set out certain information and comply with prescribed requirements. For example, the request must set out the purpose for which consent is sought and:

- The name by which the person seeking consent carries on business, if different from their name, or if not, the name of the person seeking consent.
- If the consent is sought on behalf of another person, the name by which the person on whose behalf consent is sought carries on business, if different from their name, or if not, the name of the person on whose behalf consent is sought.
- If consent is sought on behalf of another person, a statement indicating which person is seeking consent and which person on whose behalf consent is sought.
- The mailing address and either the telephone number (with access to agent or voice messaging system), email address or web address of the person seeking consent or the person on whose behalf consent is sought.
- A statement indicating that the person whose consent is sought can subsequently withdraw their consent.

Consent from recipients who are representatives of companies may be implied under CASL in certain circumstances, including where a CEM recipient has:

- Conspicuously published an electronic address that is not accompanied by a statement indicating a wish not to receive unsolicited CEMs, and the sent message is relevant to the recipient's business, role, functions or duties in a business or official capacity.
- Disclosed an electronic address to a sender without indicating a wish not to receive unsolicited CEMs, and the sent message is relevant to the person's business, role, function or duties in a business or official capacity.

The CRTC's position on "relevant to the person's business, role, function or duties in a business or official capacity" is nuanced and should be reviewed before relying on this form of implied consent.

CASL also permits implied consent to be used with both individual and company recipients where there is an "existing business relationship" or an "existing non-business relationship". These terms are specifically defined under CASL to cover customers, prospective customers and parties to contracts, subject to prescribed requirements and time limitations.

FORM AND CONTENT REQUIREMENTS

CEMs must also comply with specific form and content requirements set out in CASL and its regulations.

For example, the sender of a CEM must ensure that its message includes the following information:

- The name by which the person sending the message carries on business, if different from their name, or if not, the name of the person.

Reproduced from Practical Law, with the permission of the publishers. For further information visit practicallaw.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2016. All Rights Reserved.

- If the message is sent on behalf of another person, the name by which the person on whose behalf the message is sent carries on business, if different from their name, or if not, the name of the person on whose behalf the message is sent.
- If the message is sent on behalf of another person, a statement indicating which person is sending the message and which person on whose behalf the message is sent.
- The mailing address and either the telephone number (with access to agent or voice messaging system), email address or web address of the person seeking consent or, if different, the person on whose behalf consent is sought.
- An appropriate unsubscribe mechanism.

If it is not practicable to include the information above and the unsubscribe mechanism in a CEM, that information may generally be posted on a webpage provided it is readily accessible by the CEM recipient, at no cost, by means of a link that is clearly and prominently set out in the message.

EXEMPTIONS

CASL contains a number of exemptions to its anti-spam provisions.

Exemptions to the consent, form and content requirements under CASL. The majority of these exemptions can be found in the Electronic Commerce Protection Regulations (*81000-2-175 (SOR/DORS)*) developed and brought into force by Industry Canada, through the Governor in Council.

Some of the exemptions available under this category include:

- Messages sent by an employee, representative, or consultant of the sender to another employee, representative, or consultant within the sender, and the message concerns the activities of the sender.
- Messages sent by an employee, representative, or consultant of the sender to another employee, representative, or consultant of another organisation if the two organisations have a relationship, and the message concerns the activities of the organisation to which the message is sent.
- Messages sent in response to a request, inquiry or complaint or is otherwise solicited by the person to whom the message is sent.
- Messages sent to a person to:
  - satisfy a legal or juridical obligation;
  - provide notice of an existing or pending right, legal or juridical obligation;
  - enforce a right, legal or juridical obligation ; or
  - enforce a right arising under the law.
- An inquiry or application sent to an individual or organisation engaged in a commercial activity, where the message only constitutes an inquiry or application about that commercial activity.

The exemptions are carefully worded, and the CRTC's interpretation of these exemptions is nuanced and should be reviewed before relying on an exemption.

Exemptions to CASL's consent requirements. This category of exemptions requires that CASL's form and requirements in relation to content be followed, but does not require compliance with CASL's consent requirements.

Some of the exemptions available under this second category include CEMs that solely:

- Provide a quote or estimate for the supply of a product, goods or a service in response to a request by the recipient.
- Provide warranty information, product recall information or safety or security information to a recipient who has purchased goods or services.
- Facilitate, complete or confirm a commercial transaction that the CEM recipient had previously agreed to enter into with the person who sent the CEM or the person, if different, on whose behalf it is sent.
- Provide factual information about a product or service offered under a subscription or similar basis.
- Provide information directly related to an employment relationship or related benefit plan.
- Deliver products, goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that they had previously entered into with the sender.

OTHER RESTRICTIONS

CASL has amended the Personal Information Protection and Electronic Documents Act (*S.C. 2000, c.5, as amended*) (PIPEDA). As a result of the amendments, PIPEDA prohibits the use of computer programs to automatically collect electronic addresses (the practice known as email harvesting). This prohibition is separate from the prohibition in PIPEDA against using electronic addresses collected through email harvesting.

Through the CASL amendments, PIPEDA also prohibits the unlawful use of computer systems to collect personal information. This prohibition is separate from the prohibition against using personal information that has been unlawfully collected through the use of a computer system.

CASL has also amended part of the Competition Act (*R.S.C. 1985, c. C-34, as amended*). As a result of the amendments, the Competition Act now prohibits false or misleading representations in specific locations

Reproduced from Practical Law, with the permission of the publishers. For further information visit practicallaw.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2016. All Rights Reserved.

of an electronic message, including in the sender description, subject matter field or message field, as well as in a URL or other locator contained in an electronic message or on a website.

The Competition Bureau, which enforces the Competition Act, heavily enforces the misleading advertising provisions.

5. How does national law regulate direct marketing by text messaging (SMS)?

Direct marketing by text messaging (SMS) is regulated under CASL and direct marketing text messages are considered CEMs (see *Question 4*).

While the requirements for text messaging are generally the same as the requirements for email and other electronic communications, the CRTC has issued guidance that addresses the requirements for complying with disclosure and unsubscribe requirements in respect of text messages given the limited space available on the SMS platform.

6. How do your national data protection regulations impact on direct marketing campaigns? Please distinguish between different means of communication if different rules apply.

PIPEDA applies to the collection, use and disclosure of personal information collected in the course of commercial activity in the private sector in provinces in Canada that have not enacted substantially similar legislation.

Direct marketing campaigns that take place in a province other than Alberta, British Columbia or Quebec must comply with PIPEDA.

In addition, PIPEDA applies to federal works, undertakings and businesses (for example, airlines, financial institutions, radio and television broadcasting and broadcast distribution undertakings, and telecommunications companies), including to those that operate solely in the provinces of Alberta, British Columbia or Quebec.

Direct marketing campaigns that take place in these provinces must comply with the applicable provincial legislation:

- Alberta: the Personal Information Protection Act (*S.A. 2003, c. P-6.5, as amended*) (Alberta PIPA).
- British Columbia: the Personal Information Protection Act (*SBC 2003, c 63, as amended) (BC PIPA*).
- Quebec: An Act respecting the protection of personal information in the private sector (*RSQ, c P-39, as amended*) (Quebec Act).

7. What sanctions exist for breach of unsolicited marketing communications legislation?

The CRTC enforces the UTRs through administrative monetary penalties (AMPs).

Under the Telecommunications Act, every contravention of a prohibition or requirement under the UTRs constitutes a violation with the following penalties:

- An AMP of up to CAD$1,500 per violation for individuals.
- An AMP of up to CAD$15,000 per violation for corporations.

Under the Telecommunications Act, a breach that is continued on more than one day constitutes a separate breach in respect of each day during which it is continued.

From time to time, the CRTC makes public the nature of the contraventions, the names of the persons who commit them, and the amount of the AMPs.

Under CASL, the following penalties apply:

- An AMP of up to CAD$1 million per violation for individuals.
- An AMP of up to CAD$10 million per violation for any other person (that is, a company or any other legal entity that is not an individual).

To date, the CRTC has issued an AMP as high as CAD$1.1 million, and several organisations have agreed to make monetary payments as part of undertakings with the CRTC, ranging from CAD$48,000 to CAD$200,000.

Commencing on 1 July 2017, a private right of action becomes available under CASL. Potentially, the private right of action may be used to pursue class action law suits for CASL violations.

In April 2016, the Office of the Privacy Commissioner of Canada (OPC) issued a PIPEDA Report of Findings in respect of the electronic direct marketing practices of a company based in the province of Quebec. This was the first report of its kind. Under PIPEDA, the OPC does not have the authority to levy fines or penalties for infringements of PIPEDA. However, to ensure that the company complies with its obligations under PIPEDA, the OPC entered into a compliance agreement with the company. The matter received considerable public attention in Canada, and the PIPEDA Report of Findings and the compliance agreement are publicly available.

In June 2016, the Competition Bureau reached an agreement with two international car rental companies, and the companies agreed to pay a CAD$3 million AMP. The Competition Bureau alleged that the companies had engaged in false or misleading electronic (and other) advertising for prices and discounts on car rentals and associated products, in breach of the

Reproduced from Practical Law, with the permission of the publishers. For further information visit practicallaw.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2016. All Rights Reserved.

CASL amendments to the Competition Act (and other provisions). The prices and discounts were advertised on the companies' websites, mobile applications and in emails, as well as in certain newspaper advertisements, television commercials and flyers. In March 2015, when the Competition Bureau publicly filed an application with the Competition Tribunal in this matter, the Competition Bureau sought CAD$30 million in AMPs.

8. Please list additional national rules that may apply to direct marketing campaigns. Please explain why they apply and provide references.

Direct marketing in Canada must also comply with the general requirements of the Competition Act, which addresses false and misleading advertising, deceptive marketing practices, claim substantiation, price advertising and promotional contests.

Consumer protection legislation is enacted on a provincial basis in Canada, and direct marketing campaigns targeted towards particular provinces must comply with the consumer protection legislation applicable in those provinces. The province of Quebec in particular imposes various unique requirements, including French language requirements, restrictions on the advertising of premium offers, and registration requirements and other regulation of promotional contests.

Direct marketing campaigns targeted towards children must be mindful of certain requirements and restrictions , including a general prohibition against advertising to children in the province of Quebec.

CROSS-BORDER COMMUNICATIONS

9. Under the laws of your country, is a direct marketer bound by the laws of the country of the recipient of unsolicited commercial communication (EU principle of the country of destination)?

A direct marketer may be bound by the laws applicable in Canada, even where the direct marketer is not physically located in Canada.

10. Under the laws of your country, can an individual seek redress in their own courts against a foreign company who targeted them in breach of that individual's laws against unsolicited communications?

For breaches involving data protection, a complainant can file a complaint with the Office of the Privacy Commissioner of Canada, and once the complaint has been considered, it can seek further redress in the Federal Court of Canada.

With respect to unsolicited communications, subject to any limitation of liability imposed in accordance with the applicable statute, a person who has sustained loss or damage as a result of any act or omission contrary to the Telecommunications Act or any special Act or a decision or regulation made under either of them may, in a court of competent jurisdiction, sue for and recover an amount equal to his or her loss or damage from any person who engaged in, directed, authorised, consented to or participated in the act or omission.

An appeal from a decision of the CRTC under the Telecommunications Act on any question of law or of jurisdiction may be brought in the Federal Court of Appeal with the leave of that Court.

As noted above, a private right of action under CASL comes into effect on 1 July 2017.

SELF-REGULATION

11. Through which organisations is direct marketing self regulated in your country? Please list codes of practice if any adopted by each organisation.

The Canadian Marketing Association (CMA)'s Code of Ethics and Standards of Practice (Marketing Code) is the Canadian marketing community's self-regulation. The Marketing Code is compulsory for CMA members, and is used, from time to time, by non-members as a best practices document.

Advertising Standards Canada (ASC)'s Canadian Code of Advertising Standards (Advertising Code) contains principles of acceptable advertising generally accepted by industry and used to administer consumer complaint and trade dispute procedures. These principles and procedures can apply to direct marketing.

12. What obligations or standards do codes of practice for direct marketing impose upon marketers?

The CMA Marketing Code sets out best practices for marketing in Canada. Areas of focus in the code include:

- Overarching ethical principles.
- Universal marketing practices.
- Protection of personal privacy.
- Special considerations in marketing to children and teenagers.
- Media-specific standards of practice.

Reproduced from Practical Law, with the permission of the publishers. For further information visit practicallaw.com or call +44 20 7542 6664. Copyright ©Thomson Reuters 2016. All Rights Reserved.

The ASC Advertising Code applies to all forms of advertising in Canada, except for foreign advertising (provided the advertiser is not Canadian), political and election advertising, and packaging and labelling (which is subject to additional legislation). Areas of focus in the Advertising Code include, among others:

- Comparative advertising.
- Claim substantiation.
- Advertising to children and minors.
- Gender portrayals.
- Community standards.
- Decency and unsafe depictions.

13. Are there any opt-out lists in your country? If so, how does one register on each list? Which organisation manages each list? What rules apply to each list?

The National DNCL is an opt-out list for unsolicited telephone calls and faxes (see *Canadian Radio-television and Telecommunications Commission: national do not call list*). The National DNCL is managed by the National DNCL operator. Consumers can register telephone and fax numbers on the National DNCL by entering the numbers at the following website: *www.lnnte-dncl.gc.ca/insnum-regnum-eng*. The UTRs apply to the National DNCL.

Commercial electronic messages cannot be sent to recipients unless the sender has the express consent of the recipient, or the sender is able to rely on implied consent (as defined under CASL) or an exception under CASL (see *Question 4*). Unlike other jurisdictions, like the United States, Canada's anti-spam regime is an opt-in , not an opt-out regime. There is no centralised opt-out list for emails.

14. What procedures exist for complaining to organisations against unsolicited communications?

The following procedures exist for complaining about breaches of the direct marketing laws and codes:

- **UTRs.** Complaints may be reported to the CRTC's Complaints Investigator delegate (see *Canadian Radio-television and Telecommunications Commission: Complain about a telemarketing call*).
- **CASL.** Complaints may be reported to the Canadian Spam Reporting Centre (see *Canadian Spam Reporting Centre*).
- **The Advertising Code.** Complaints may be filed with the ASC (see *Advertising Standards Canada: How to submit a complaint*). Consumer complaints are referred to the ASC's Standards Council, which adjudicates the complaints. Trade complaints are administered through a separate confidential procedure.
- **The provisions of the Competition Act amended by CASL.** Complaints may be filed with the Canadian Competition Bureau (see *Competition Bureau: Questions and Complaints*).

Consumer protection legislation is enacted provincially in Canada. Consumer protection related complaints pertaining to a particular province may be filed with the appropriate provincial consumer protection body. For example, in the province of Ontario, consumer protection complaints may be filed with the Ontario Ministry of Government and Consumer Services (*www.ontario.ca/page/filing-consumer-complaint*).

Legal solutions from Thomson Reuters
Thomson Reuters delivers best-of-class legal solutions to help you practise the law, manage your organisation and grow your business. Our solutions include Practical Law, Westlaw UK, Sweet & Maxwell and Lawtel, and a series of software solutions including Serengeti, Solcara and Thomson Reuters Elite, intelligently connect your work and your world with our content, expertise and technologies.
Find out more at *legal-solutions.co.uk*

Compliance Preparedness Checklist for Canada's Anti-spam Legislation (CASL)

Organizations should develop a compliance preparedness checklist for Canada's anti-spam legislation (CASL) that's appropriate to their organizational structure, their operations, and other organization-specific considerations.

This checklist includes various activities an organization should consider undertaking as part of its CASL compliance efforts.

- □ Conduct an audit/gap analysis of the organization's current electronic communication practices.
- □ Determine all of the purposes for which the organization might wish to communicate electronically with someone, and which purposes require consent.
- □ Identify applicable exemptions to commercial electronic messages requirements.
- □ Turn implied consents into express consents, where appropriate.
- □ Prepare template consent language and other applicable templates.
- □ Establish opt-in consent mechanisms and consent renewal mechanisms.
- □ Ensure current status of consents for individuals and organizations (implied or express) are properly recorded in a database or other manner.
- □ If relying upon implied consents, ensure that databases or lists can manage time limits (e.g., 2 year and 6 month time limits).
- □ Document and maintain appropriate evidence of consent.
- □ Establish an unsubscribe mechanism, and then review and test how quickly it actually works.
- □ Establish an appropriate way employees, contractors, officers, directors, agents etc. can check whether a potential message recipient has "opted-out" or "unsubscribed" from receiving commercial electronic messages.
- □ Ensure that signatures/notices are used by employees, contractors, officers, directors, agents, etc. whenever an external commercial electronic message is sent, and that such signatures/notices contain all of the information required under CASL.
- □ Review contracts with all third parties, and, where appropriate, require CASL and other compliance.
- □ Consider drafting a CASL compliance policy, and keep it up-to-date.
- □ Review and update privacy policies, including a website privacy policy (where applicable), and website terms of use (where applicable).
- □ Establish policies and procedures to monitor CASL compliance.
- □ Ensure that there is on-going internal CASL education and training of employees, contractors, officer, directors, agents, etc.

- □ Ensure that employees, contractors, officers, directors, agents, etc. are, as prohibited under CASL,:
  - □ not altering transmission data in electronic messages
  - □ not installing or causing to be installed, any computer programs onto another person's computer system, or using a program after installing it to send a message, without the express consent of the owner or authorized user of the computer system
  - □ not making false or misleading statements in commercial electronic communications
  - □ not using computer programs to automatically collect electronic addresses (i.e., "email harvesting")
  - □ not using electronic addresses that have been collected through "email harvesting"
  - □ not unlawfully using computer systems to collect personal information
  - □ not using personal information that has been unlawfully collected through the use of a computer system
- □ Conduct regular technical audits/reviews of the organization's computer systems (including mail servers) to ensure that an unauthorized third party hasn't gained access to them, and isn't using them to send out non-CASL compliant commercial electronic messages.
- □ Review options for appropriate directors' and officers' liability insurance.

About the Author:

J. Andrew Sprague is a Professional Support Lawyer in the Toronto office of Baker & McKenzie LLP, a global law firm. He can be reached at 416.865.2344 or andrew.sprague@bakermckenzie.com.

This checklist is provided as an information service, and the information contained in this checklist is not meant as legal advice or opinion. Readers are cautioned not to act on information provided in this checklist without seeking specific legal advice with respect to their unique circumstances.

Canada's Anti-spam Legislation (CASL) - Electronic Communications Survey

The first step of any CASL compliance plan is to audit an organization's current electronic communications practices.

It may be necessary to survey various departments to get a full picture of an organization's activity.

There are a number of questions an organization should ask itself when undertaking an audit. These questions will enable an organization to determine the issues that must be addressed in order to bring itself into compliance.

1. What forms of electronic communications does the organization use to communicate with internal and external parties? (e.g. email, instant messaging, text messaging/SMS, social networks (e.g. Facebook®, LinkedIn®, Twitter®), other electronic services)

2. On behalf of which entities does the organization send out electronic communications? (e.g. identify primary organization and any related or affiliated organizations)

3. To whom does the organization send external electronic communications? (e.g. clients/customers, potential clients/customers, volunteers, members, landlords and/or subtenants, government/quasi-government bodies, vendors, suppliers)

4. For each of the communications media listed in Question #1, what identifying information about the primary organization, or one of its related or affiliated entities, is included with each message? (e.g. do you use email signatures or other identifiers? What information is included?)

5. Does the organization presently request consent to send electronic communications to recipients? If yes, how are these requests made and recorded?

6. Does the organization track the manner in which the contact information of recipients of its messages is received by the organization? (e.g. whether the organization obtained the information from a business card, email, program/event registration, referral)

7. Does the organization add its contacts to a contacts list, database, or customer relationship management (CRM) software?

8. Are email addresses collected through means of an email address harvesting program (either directly or indirectly)?

9. Does the organization purchase any email address lists from third parties? If yes, who are the lists purchased from, how are they collected, and what does the organization do with the email addresses that it purchases?

10. Does the organization rely on any third parties to communicate electronically on its behalf? Do third parties send out emails or social media messages on behalf of the organization?

11. Does the organization perform any electronic messaging on behalf of third parties or make available any email addresses to third parties? If yes, why does the organization make such email addresses available and what do the third parties do with such email addresses?

Consent is also required if transmission data is altered in an electronic message or if a computer program is installed on another person's computer in the course of commercial activity. If an organization engages in these activities, there are additional questions that should be asked.

About the Author:

J. Andrew Sprague is a Professional Support Lawyer in the Toronto office of Baker & McKenzie LLP, a global law firm. He can be reached at 416.865.2344 or andrew.sprague@bakermckenzie.com.

This checklist is provided as an information service, and the information contained in this checklist is not meant as legal advice or opinion. Readers are cautioned not to act on information provided in this checklist without seeking specific legal advice with respect to their unique circumstances.